NAVAL WAR COLLEGE
Newport, R. I.

Information Should be an Operational Factor of War in the Information Age.

by

Kevin D. Bohnstedt
LCDR USN

A paper submitted to the Faculty of the Naval War College in partial satifaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: Kevin D Bohnstedt

7 February 1997

Paper directed by
CAPT G. Jackson
Chairman, Department of Joint Military Operations

Wayne F. Sweitzer 6FEB97
CDR W. F. Sweitzer Date
Faculty Advisor

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification): Information Should be an Operational Factor of War in the Information Age. (U)

9. Personal Authors: LCDR Kevin D. Bohnstedt, USN

10.Type of Report: FINAL

11. Date of Report: 7 February 1997

12.Page Count: 27

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:
Operational Factors
Information
Information Age
Netwar/Cyberwar
Information Operations
Operational Art

15.Abstract:

Over the past five years, numerous articles have been published prophetically evaluating the future battlespace, and what forces will be used to fight in that space. Although there has been no firm direction yet drawn on where this "Revolution in Military Affairs" (RMA) will lead us, it will surely change military practices, doctrines, and basic precepts.

Historically, time space, and forces have been considered the operational factors of war. While their importance is due to the freedom of action they provide when used in the correct balance, information has always played a pivotal role in effectively achieving the correct balance. Further, all Joint Warfighting Publications recognize information domination or superiority as a basic tenet of the future of warfare.

This paper proposes that with the military poised on the brink of the information explosion and RMA, information should takes its rightful place as the fourth operational factor of war. This concept is examined from the perspective of collection, management, utilization, exploitation, and security.

16.Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461

20.Office Symbol: C

ABSTRACT

Over the past five years, numerous articles have been published prophetically evaluating the future battlespace, and what forces will be used to fight in that space. Although there has been no firm direction yet drawn on where this "Revolution in Military Affairs" (RMA) will lead us, it will surely change military practices, doctrines, and basic precepts.

Historically, time space and forces have been considered the operational factors of war. While their importance is due to the freedom of action they provide when used in the correct balance, information has always played a pivotal role in effectively achieving the correct balance. Further, all Joint Warfighting Publications recognize information dominance or superiority as a basic tenet of future warfare.

This paper proposes that with the military poised on the brink of the information explosion and RMA, now is the time for information to takes its rightful place as the fourth operational factor of war. This concept is examined from the perspective of collection, management, utilization, exploitation, and security.

Information Should Be an Operational Factor of War in the Information Age

I. Introduction

> "The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeros, little bits of data. It's all just electrons. ...There's a *war* out there...A *world war*. And it's not about who's got the most bullets. It's about *who controls the information*."[1]

The recent boom of computer and information based networks on the worldwide markets has led to an explosion of computer based technologies and capabilities that is commonly referred to as the "Information Age." The main thoroughfare through this network of systems, the "Information Superhighway," has reaped impressive benefits in linking all areas of the world. From the Internet to CNN's worldwide instantaneous reach, the global presence of information as a commodity is causing forward looking thinkers to reevaluate past truths, where the world is going, and what it will look like in ten years. The linking of these information structures or "Infosphere"[2] and expanded reliance on computers is also sending shock waves through the military.

Over the past five years numerous articles have been published prophetically evaluating the future battlespace, and what forces will be used to fight in that space. Although there has been no firm direction yet drawn on where this "Revolution in Military Affairs" (RMA)[3] will lead us, it will surely change military practices, doctrines, and basic precepts. Some theorists believe the RMA will manifest itself in greatly reduced numbers of forces required to wage a war of long range information-based weapons while others think it will just enhance the commanders ability to "see"

the battlespace and control every aspect of the battle.[4] Admiral William Owens, former Vice Chairman, Joint Chiefs of Staff, goes as far as defining this new playing field as a "system of systems."[5] The late Admiral Mike Boorda, former CNO, put this RMA in perspective in a recent article

> We are in a revolution of no less importance than the advent of steam propulsion, carrier aviation, or nuclear submarines. The so-called revolution in military affairs has moved information and the need for information dominance to center stage in thinking about warfare. Development of advanced information and communications technologies will continue. Successful implementation of these innovations requires their integration into force structure and operational concepts.[6]

As these Admirals point out, this revolution will open new avenues of thought on widely held concepts. Leaders throughout the military recognize this revolution and are adjusting through new concepts such as netwar, cyberwar, the predominance of Information Warfare (IW), and a new area of concern -- Information Operations (IO).[7] With these new avenues in mind, reevaluating the basic theory of Operational art is required.

II. Thesis

> How we respond to dynamic changes concerning potential adversaries, technological advances and their implications, and the emerging importance for information superiority will dramatically impact how well our Armed Forces can perform its [sic] duties in 2010.[8]

Some authors propose that the fourth generation of war has arrived. The preceding three "focused, in turn, on massed manpower, then massed firepower, and finally on maneuver."[9] The contention is that these shifts in emphasis are driven by changes in "political, social, and economic factors."[10] Although technology led the way to the information age, and RMA, the current shift in focus towards a fourth generation goes deeper. Extensive political changes on the world stage brought about by the end of the iron curtain and the growing world perspective all nation states are

gaining coupled with the burgeoning international networks linking societies both socially and economically are the true driving factors behind this paradigm shift.[11] This networking of all players on the world stage, and interdependency on the networked world have given the transfer and control of information a truly new importance.

Part and parcel of this new networked capability is expanding battlespace situational awareness to a full force level. With the leaps in technology currently in place and the forward thinking of our military leaders, our ability to see and shape this battlespace is becoming a main topic of concern. Using worldwide networking capabilities, the time required for reaction to current crises throughout any operation is dramatically shorter. Whereas the time to evaluate and respond to crises have historically been hours to days, Desert Storm shortened that span to minutes. With the current networked transfer rates and battlespace awareness, the capability for instantaneous evaluation and response is here.[12] The overarching commodity then becomes the control of the information transferred.

Historically time, space, and forces have been considered the operational factors of war.[13] While their importance is due to the freedom of action they provide when used in the proper balance information has historically played a pivotal role in effectively acheiving the correct balance. With the advent of the information age and the greatly increased importance of controlling information in military operations, it is time that the fourth critical operational factor, information, is added to this list. How we collect, manage, utilize, exploit, and secure information to optimize the three

traditional factors is paramount to the discussion of this paper. These balancing tools will be analyzed with respect to the historic examples of the Falklands conflict and Desert Storm as well as proposed future capabilities.

III. Common Ground

The most important aspect in attacking this problem is defining the terms--coming to a common ground. Specifically the definition of "information" is the linchpin. Current Joint Pubs contain the most restrictive definitions, but each service also defines these terms independently. Further, the terms netwar and cyberwar, while written about prolifically have not been added to the approved military lexicon. "While no current definition is satisfactory, as a rule many analysts subscribe to a hierarchy with data at the bottom, information in the middle, and knowledge at the top (some would add wisdom above that)."[14] This cognitive hierarchy, as shown in Joint Pub 6-0, NDP-6, and FM 100-6 is the commonly accepted standard for the discussion and definitions of data, information, and knowledge. The following paragraphs will contrast these differences in these definitions.

Information

Although the Joint Pubs differ in their definitions of information, Joint Pub 3-13.1 (the most recently published) describes information as, "facts, data, or instructions in any medium or form."[15] Previous Joint Pubs add, "the meaning that a human assigns to data by means of the known conventions used in their representation."[16] FM 100-6 defines information as "data collected from the environment and processed into a usable form."[17] While it is important to recognize

the similarities in these definitions, their differences need to be reckoned with as well. They do not include the processing capabilities, but what is processed. This will allow for future collection and processing capabilities. Importantly though, they all include the facet that the data has been processed and given meaning. Analysis and collation are performed at a higher level. Thus, this paper will use the following definition; processed data, facts, and instructions with the meanings we apply to those items.

Information Warfare

This definition is universally agreed to in service specific pubs and Join Pubs.

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. Also called IW.[18]

FM 100-6 has recently defined IW as a subset of information operations. Further, it has placed Command and Control Warfare (C2W) as a subset of IW.[19]

Netwar and Cyberwar

Netwar is "trying to disrupt, damage, or modify what a target population 'knows' or thinks it knows about itself and the world around it."[20] Cyberwar on the other hand, "refers to conducting or preparing to conduct military operations according to information-related principles."[21] The major differences between these two concepts is that netwar is oriented primarily towards nonviolent to low intensity conflict while cyberwar refers more to conduct of that war, and can apply throughout the spectrum of war.[22] Netwar would affect the information the population received and their beliefs while cyberwar would target the way they received this information.

In context, through the spectrum of war, these two offensive mindsets would be combined with defensive ploys to produce IW, each focusing on its specific aspects.

Operational Art

Joint Pub 3-0 defines this term as

> The employment of military forces to attain strategic and/or operational objectives through the design, organization, integration, and conduct of strategies, campaigns, major operations, and battles. Operational art translates the joint force commander's strategy into operational design, and, ultimately, tactical action, by integrating the key activities of all levels of war.[23]

Traditionally this art form has included the orchestration of all operational actions, factors, and considerations into a comprehensive plan to achieve strategic objectives. Essentially, it bridges the gap between the tactical world and the strategic. Thus the operational commander controls all aspects of the campaign from inception of the design to the post hostilities phase.

Operational Factors

Traditionally three things have been considered operational factors. These three items are "time, space, and forces."[24] These three items and the permutations of their combinations allows the operational leadership to establish a framework to seize the initiative, maintain freedom of action, and achieve the strategic goals set before it. The framework set in place will include how these items affect each other and what effect this will have on the final outcome, or the path to get to that final outcome.[25] The artistry of orchestrating these factors will determine the ability to maintain freedom of action. This freedom of action is the most crucial concept they provide.

IV. The Current Balancing Act

> "Strategy is the art of making use of time and space. I am in less charge of the latter than the former. Space we can recover, lost time never." Napoleon I Bonaparte[26]

> "Superior force is a powerful persuader." Winston Churchill, Note to the First Sea Lord, 15 October 1942.[27]

While the three historic factors of war by themselves require intensive planning and management, their synergistic effects are the aspects the operational commander is seeking. Used properly, these factors will allow the commander to seize the initiative. This initiative will directly result in enhanced freedom of action. Truly this freedom of action is the crux of the results from these factors of war. The operational commander, from plan to execution must strive to use each of these to their best advantage. Always mindful of their effects on the others and more importantly on the progress to the final goal.

V. Information as a factor

> In many respects, one can consider information as a realm, just as land, sea, air, and space are realms. Information has its own characteristics of motion, mass, and topography, just as air, space, sea, and land have their own distinct characteristics. Before the Wright brothers, air, while it obviously existed was not a realm suitable for practical, widespread military operations. Similarly, information existed before the Information Age. But the Information Age changed the information realm's characteristics so that widespread military operations within it became practical.[28]

The Joint Pubs and Joint Vision 2010 continually make reference to obtaining and maintaining information dominance or information superiority over adversaries. The desire to gain this information differential is the basis for the future of success in warfare. How to achieve and maintain this information differential is the crux of the discussions in RMA. Whether through netwar, cyberwar, or some unforeseen new capability that will be used in the next conflict, the requirement for maintaining a dominance in information over adversaries is essential.

This desire for information dominance is not a new concept. Practitioners have used information dominance strategies since the time of the Mongols in the 12th and

13th centuries when Mongolian warriors defeated far superior forces in their campaign against the Muslim empire of Khwarezm. By seeking out where the enemy was, and more importantly where he wasn't, the Mongols worked around the enemy lines and intercepted all messengers advising the Khwarezm ruler of their positions. Hence, Mohammed Ali Shah, the Khwarezm ruler was operating blind and thought all was well. When a messenger finally did get through, the Mongols were less than a day away. Mohammed Ali Shah could not maneuver his troops to the proper place in time to do battle. Thus his lack of information clearly restricted his freedom of action. The ruler fled and the army was defeated.[29]

While this "information dominance has always 'mattered,'...a variety of factors have now converged to enable it to fulfill its potential to achieve overarching effects in the realm of conflict."[30] These new "factors" are the new networking capabilities and new battlespace management concepts. This capability to capitalize on the informational differential will allow the operational artist of the future to climb inside and run the opponent's decision cycle. The concept of a decision cycle is presented in Joint Pub 3-13.1. It alludes to adjusting the so-called Observe, Orient, Decide, and Act (OODA) loop.[31] By affecting this OODA loop, a commander on the future battlefield will be able to define his own freedom of action. GEN Sullivan published his idea of currency of command in which the OODA loop has evolved from hours and days to the present capabilities of real time Observations, continuous Orientations requiring immediate Decisions, with follow on Actions within an hour.[32]

So how can information provide the freedom of action so vital to the definition of an operational factor? This investigation needs to center on the basic balancing tools the commander should use throughout the campaign.

Collection

Having the correct information collected is paramount to the commander's ability to correctly drive the campaign in the proper direction. Due to proposed future capabilities as well as those not yet foreseen, future collection capabilities become difficult to predict. As Joint Pub 6-0 shows, the future architecture of the Global Command and Control System (GCCS) networked to the interoperable systems of all services will create the Command, Control, Communications, Computer, and Information For The Warrior (C4IFTW) concept. This will allow everyone from the strategist to the warrior in the field to be able to see the battlespace, attain a "global understanding," and optimize it to their maximum potential.[33]

While the specific capabilities to perform this aren't yet known, the forces necessary to set up these systems, run them, and analyze the information attained from them will always be necessary. The time to set up these systems if they do not exist in theater must be allowed. The other attribute necessary to consider will be the space they will require. This may take away from the space available to supporting structures for the battlefield participants. While hopefully the architectures will be autonomous and included in all aspects of the individual services, logistic planning for it must be considered. This information collection capability also drives follow-on operations of the campaign. Every avenue to gain information must be explored and

utilized. Some of these include the media, civil authorities, political advisors, and host nationals if available.

Further, the commander must decide what information is critical. The current drive towards a "pull system" where everything available on the area is accessible vice the "push system" where he is given what others think is important helps alleviate problems with overloading. In setting up the system, however, the analyst must be knowledgeable of what is available. If the analyst does not have intimate knowledge of what is available -- its quality, accuracy, and timeliness -- he will not have the time to produce the necessary information. This will drive a paralysis by analysis. This paralysis will seriously hamstring the operational actions of the forces and lose crucial reaction time.

Historically, the lack of a sufficient collection capability severely hampered the Argentinean capability to design its branches and sequels in its air battles during the 1982 Falklands war. Arguably the operation had no specific extensive long range design, but the fact that command and control pipelines were "stovepiped" inside each service, and returning aircraft debriefs were not given to a centralized collection arena effectively made the forces employed blind and provided no guidance for what to attack next. This lack of guidance for follow-on actions suboptimized the use of the long range punch available from these aircraft. As they were operating at the edge of their range, they were limited to targets of opportunity vice a coordinated effort. On the counterpoint, the British knew where the Argentines would be coming from, and although they had no early warning aircraft, they responded by keeping their carrier

out of range for Argentine attack, but close enough for quick response.[34] By appropriately balancing space versus the attacking forces limitation of range, the British maintained their freedom of action in the absence of crucial information.

During Desert Storm however, the network established to support the operation was the "largest in history."[35] "In addition to equipment differences among various Coalition members, there were differences among US forces...At the height of the operation, this hybrid system supported more than 700,000 telephone calls and 152,000 messages a day."[36] This amazing system, set up from disparate sources, worked beautifully because of the logistic support and time allowed to make it work.[37] Without this, the information required to support this operation would not have been available. Additionally, the Joint Surveillance Target Attack Radar System (JSTARS) was employed to provide real time information on the battlespace. This information became crucial at the beginning of the ground offensive.[38]

Management

The management of information is key to the success of any operation. As alluded to earlier, C4IFTW should allow the quick transfer of instructions and information to the people who need it. Currently, FM 100-6 lists an information operations cell that closely resembles the C2W cell suggested in Joint Pub 3-13.1. This cell is run by the J3, includes the J6, J2 , J5, public affairs representative, and other planners. The parts of this cell not addressed that need to be included are the State Department representative, Civil Affairs Representative, and any Host Nation representative. This will make this cell more useable throughout the spectrum of war.

By deriving what information is necessary, collecting it, and distributing it as required, this cell will optimize performance of all forces assigned.

What does this management cell provide the commander? It allows him to plan for the scheme of information dominance to use in the field, employ it, and evaluate the information collection for follow-on operations. Getting this information early and accurately is crucial to putting out a clear vision of how things are to run. This scheme of operations will synchronize the multiple forces employed and sequence their actions in time and space. Without this overarching design, the forces will not be employed in the most advantageous situation. Their capability to gain and maintain their own freedom of action will be restricted.

As shown above, the Argentines lack of management of information suboptimized their forces. Further, the British press onboard the Operation Corporate Task Force had heard the Argentine bombs did not explode on impact. This vital information was withheld from the printers so the Argentine forces would not be alerted to this problem. The Naval forces was using shorter fuse settings and retarded fins to allow for successful low altitude bomb runs, while the Air Force was not. The lack of a sufficient management system to share this information caused this disparity. Had this been resolved, the problem of the dudded bombs would have been averted.[39]

Recently, GEN Zinni described the "stovepiping" of information during the Operation Restore Hope actions in Somalia. Each separate service and force coming in to help had its own structure set up, and had collected different bits of information.

What this led to was a diverse purpose in the operation, and the forces not being able to capitalize on the correct information necessary to maintain their freedom of action.[40]

Utilization

Once the information has been collected, and the management team has been assembled to manage it, then what? The information available to the commander will be used to set up his plan for the scheme of the operation. As stressed in the Commander's Estimate of the Situation structure, this initial information is perhaps the most important to the success of the mission.[41] Without correct, accurate, and complete information, the commander will be hamstrung in his ability to provide his "vision" of the operation to his subordinates. This lack of information, and more important, instruction on the design of the operation will disallow the forces from positioning themselves to gain and maintain their freedom of action. The requisite synergy obtained by sequencing and synchronizing forces in time and space will be sacrificed. FM 100-6 stresses this proper utilization of information as driving the situational awareness of all players in the campaign.[42]

Historically, the utilization of information to gain freedom of action while restricting the adversary's is documented even by GEN George Washington. Peter Stevens chronicles Washington's use of *dis*information during the bitter winter of 1776-77. He hid the sad state of the Continental army from GEN Howe by stationing two to three soldiers in every mansion and house over a wide area so that whenever anyone was in the area, it appeared that he had many more troops than he did. Concurrently, he made up rolls showing that he had 12,000 troops vice the 4,000 he

actually had. In a convincing ploy, he allowed the British to get this information via separate channels. Once Howe received this information, he decided that the number of forces was too great to attack, and that "saved us thro' the winter."[43] While not exactly in the information age, Washington's use of information allowed him the operational pause he needed.

Closer to this age, the overall plan during Desert Storm was to use airborne assets to destroy Saddam Hussein's capability to see the battlespace and direct his forces by destroying his command and control nodes, and Integrated Air Defense Systems (IADS). This allowed coalition forces to maintain air superiority, and blinded him to the overarching design of moving massive amounts of forces quickly to the west. This, coupled with continual media reports of Amphibious Task Forces (ATFs) preparing for an amphibious assault and a feint at the beginning of the ground campaign tied Iraq's forces to the coast.[44] Without this comprehensive plan to deny information to Iraq this orchestrated maneuver would not have been possible.

Exploitation

FM 100-6 defines exploitation as "'taking full advantage of any information that has come to hand for...military operational purposes.' All information environments and systems surrounding an operation, friendly and adversarial, military and nonmilitary, offer chances for exploitation."[45] This quote gets right to the heart of the idea. While the other areas of information-based warfare ideas wind around a process or an architecture, the utilization, more specifically the *exploitation* of a lack

of information or a disinformation campaign is where the true freedom of action can be obtained.

The desired effect is to affect the adversary's decision cycle. To deny the opposition information while maintaining your own information requirement, and exploiting that differential correctly, will surely lead to success. The area of C2W, netwar, and cyberwar provide a comprehensive list of ways to exploit information differentials. Some of the universally accepted methods of exploitation in C2W are deception, psychological operations (PSYOPS), physical destruction, electronic warfare (EW), and operations security (OPSEC). However, if the capability to exploit disinformation in the media are included, this becomes a more complete list.

To see how the use of exploitative measures provides freedom of action, one could look to the previous example of the deception campaign in Desert Storm. Through the denial of necessary information to the Iraqi leadership, fully 100,000 troops and 1,200 tanks were transported through the desert to attack from the west. This surprising move caught the Iraqi troops in a position they were unable to defend.[46] Part and parcel to the success of this maneuver however was that Iraq had expected a landing from the Persian Gulf by the embarked MEB. By exploiting the Iraqi's lack of information on troop concentrations and introducing a deceptive plan, the coalition gained the required freedom of action to employ the "Hail Mary" plan.

To add to this deception operation, the 4th Psychological Operations Groups (POG) deployed to the Persian Gulf. Their target was "the preconceived fears and concerns of Iraqi soldiers in both front and rear areas."[47] To accomplish this, they

dropped 29 million leaflets and conducted loudspeaker operations throughout the conflict.[48] This was designed to affect the will to fight by praying on the lack of countering information given to the basic Iraqi soldier.

Security

For any of these information designs to succeed, the utmost security must be maintained. The deception campaigns during World War II required not only plausibility, and thorough execution, but strict security to make them work.[49] Specifically, if the operational commander cannot trust the information he has at hand, he will not be able to utilize it to his best advantage. Once compromised, this information is then suspect for the rest of the operation. Without that requisite information, the commander is essentially blind. The enemy could easily be controlling his decision cycle. This situation will specifically lose the freedom of action the operational commander wishes to gain. In the networked world, this concept becomes even more important. The fact that a computer "hacker" could slightly alter bits of data in national databases and present a skewed picture to national authorities becomes a frightening idea. This hacker may be acting as an agent from some faction of a terrorist organization, or other country. Either way, the inherent necessity for thorough security becomes self evident.

VI. Conclusions

Throughout history, information, or more importantly the control of information has been an important facet of war. Although the structures and capabilities have not been available in the past to legitimize this commodity as a factor

of war, recent initiatives have vaulted it to its proper place in the hierarchy of operational considerations. Poised on the brink of the biggest revolution in military thought in recent history, the prudent operational artist will anticipate the next generation of warfare and include information as the fourth operational factor of war now.

NOTES

[1] "Sneakers", VHS, 2 hrs. 5 mi[illegible] 1993, MCA Universal Home Video, Inc. Character Cosmos is speaking to Marty Bishop at the end of the movie.

[2] Chairman, Joint Chiefs of Staff, Doctrine for Command, Control, Communications, and Computer Systems Support to Joint Operations, Joint Pub 6-0, Washington, D. C., 1995, II-1.

[3] Many authors have pontificated about the RMA. The phrase has become a standard among forward thinking military professionals.

[4] The specifics of the "RMA" aren't clearly defined. While some authors believe it will manifest itself in highly technical weapons and perhaps reduce the numbers of forces involved, others think it will just enhance our "vision" of the battlespace. Still others think it will combine these two attributes and truly expand the operational reach of the battlefield. Regardless of the author, all call for new innovative thoughts and re-examination of the basic precepts of waging war.

[5] ADM William A. Owens, "Emerging System of Systems," Proceedings, May 1995, 35.

[6] ADM Jeremy M. Boorda, "Leading the Revolution in C4I," Joint Force Quarterly, Autumn, 1995, 14.

[7] Netwar and cyberwar are phrases commonly used today which were introduced by John Arquilla and David Ronfeldt in their thinkpiece "Cyberwar is coming!" published by the RAND corporation in 1992. IW is an area that has gotten a great deal of attention in the past few years. Information Operations has recently been formalized in the U. S. Army's manual FM 100-6, Information Operations.

[8] Chairman, Joint Chiefs of Staff, Joint Vision 2010, Washington, D. C., 1994, 8.

[9] LtCol Thomas X. Hammes, "The Evolution of War: The Fourth Generation," Marine Corps Gazette, September 1994, 35.

[10] Ibid.

[11] Ibid, 35-36.

[12] GEN Gordon R. Sullivan, and James M. Dubik, War in the Information Age, Carlisle Barracks PA, Strategic Studies Institute, U. S. Army War College, 1994, 5. This point is graphically made in a figure on the currency of command in relation to decision cycles.

[13] Milan Vego, "Operational Art," Unpublished Class Manual (NWC 4090), U. S. Naval War College, Newport RI, 1996, 6.

[14] John Arquilla and David Ronfeldt, "Cyberwar is Coming!", Santa Monica, CA, RAND, 1992, 5.

[15] Chairman, Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Pub 3-13.1, Washington, D.C., 1995, GL-8.

[16] Chairman, Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to Operations, Joint Pub 2-0, Washington, D. C., 1995, GL-8.

[17] U. S. Department of the Army, FM 100-6, Information Operations, Washington, D. C., HQ, Department of the Army, 1996, 2-1.

[18] Chairman, Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Pub 3-13.1, Washington, D. C., 1996, GL-8.

[19] This idea is graphically presented on a slide presented during a lecture at the Naval War College by CDR Lee Ducharme, Nov 96.

[20] John Arquilla and David Ronfeldt, "Cyberwar is Coming!", Santa Monica, CA, RAND, 1992, 5.

[21] Alan D. Campen, "Rush to Information-Based Warfare Gambles with National Security," Signal, July 1995, 68.

[22] These concepts are originally brought up in John Arquilla and David Ronfeldt's thinkpiece "Cyberwar is Coming!", and further discussed in Alan D. Campen's article "Rush to Information-Based Warfare Gambles with National Security." Recently many papers have begun to try to further define and refine these terms and how they apply to military operations. To date, there has been no official adoption of these concepts or induction into the official military lexicon.

[23] Chairman, Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Pub 3-0, Washington D. C., 1995, GL-10.

[24] Milan Vego, "Operational Factors," Unpublished Class Manual (NWC 4092), U. S. Naval War College, Newport, RI, 1996, 1.

[25] This concept is further discussed and presented in Professor Milan Vego's "Operational Factors" manual used at the Naval War College.

[26] As quoted in Milan Vego, "Operational Factors", Unpublished Class Manual, (NWC 4092), U. S. Naval War College, Newport, RI, 1996, 1.

[27] Ibid., 27.

[28] U. S. Department of the Air Force, Cornerstones of Information Warfare, Washington, D. C., 1995, 8-9.

[29] John Arquilla and David Ronfeldt, "Cyberwar is Coming!", Santa Monica, CA, RAND, 1992, 11.

[30] John Arquilla, "The Strategic Implications of Information Dominance," Strategic Review, Summer 1994, 27.

[31] Chairman, Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare, Joint Pub 3-13.1, Washington, D. C., A1-A2.

[32] GEN Gordon R. Sullivan and James M. Dubik, War in the Information Age, Carlisle Barracks, PA, Strategic Studies Institute, U. S. Army War College, 1994, 5.

[33] This concept is presented in chapter II of Joint Pub 6-0.

[34] Harry D. Train, II, "An Analysis of the Falkland/Malvinas Islands Campaign," Naval War College Review, Winter 1988. The lack of a consistent chain of command, and unity of purpose is addressed throughout.

[35] Conduct of the Persian Gulf War, as quoted in Joint Pub 6-0, III-6.

[36] Ibid.

[37] This system is alluded to in Joint Pub 6-0, and fully discussed in Conduct of the Persian Gulf War: The Final Report to Congress, Annex K. Although the basic tools were available to construct the system, the Time-Phased-Force-Deployment-Data documents needed to be addressed to give the required time and transport space to bring all the components together. The construction of the system was truly a feat of engineering marvel that had far reaching affects.

[38] Conduct of the Persian Gulf War. The Final Report to Congress discusses the employment and value of the JSTARS in annex C, K, as well as throughout volume 1. Additionally, Alan Campen describes the capabilities and contributions in The First Information War, pp.168-170.

[39] Valerie Adams, The Media and the Falklands Campaign; and Bruce W. Watson, ed. Military lessons of the Falkland Islands War: Views From the United States. Both books allude to this. Adams states in her discourse on information of national interest on page 160. Watson mentions it with respect to the bombing of the Falklands in the discussions on "Air Power Lessons Learned," page 45.

[40] VHS presented on interview with GEN Zinni at the Naval War College.

[41] Joint Military Operations Department, "Commander's Estimate of the Situation Workbook," Unpublished Class Manual, U. S. Naval War College, Newport RI, 1996.

[42] FM 100-6, 1-11.

[43] Peter F. Stevens, "Early Disinformation Campaign," Military History, June 1992, 16.

[44] Conduct of Operation Desert Storm. Final Report to Congress, pg 344. Additionally, GENs Powell, and Schwartzkopf discussed 'poking Iraq's eyes out, and then killing it' numerous times in briefings and interviews.

[45] FM 100-6, 2-11.

[46] Joint Pub 2-0, III-7;III-9.

[47] Maj Jack N. Summe, "PSYOP Support to Operation Desert Storm," Special Warfare, Dec 1992, 9.

[48] Ibid.

[49] Charles G Cruickshank, Deception in world War II, New York, Oxford University Press, 1980. The author discusses these three tenets throughout the book in his description and analysis of the operations of World War II.

BIBLIOGRAPHY

Adams, Valerie. The Media and the Falklands Campaign. New York, NY: St Martin's Press, Inc, 1986.

Anderson, Gary W. and Terry C. Pierce. "Leaving the Technocratic Tunnel." Joint Force Quarterly, Winter 95-96, 69-75.

Arquilla, John. "The Strategic Implications of Information Dominance." Strategic Review, Summer 1994, 24-30.

_____, John and David Ronfeldt. "Cyberwar is Coming!" Santa Monica, CA: RAND, 1992.

Barriteau, Brad and CDR Lee Ducharme. "Information Operations Overview for JLASS 97" Unpublished Slides, U. S. Naval War College, Newport RI: 22 November 1996.

Boorda, ADM Jeremy M. "Leading the Revolution in C4I." Joint Force Quarterly, Autumn 1995, 14-17.

Campen, Alan D. "Information Warfare is Rife With Promise, Peril." Signal, November 1993, 19-20.

_____, Alan D. "Rush to Information-Based Warfare Gambles with National Security." Signal, July 1995, 67-69.

_____, Alan D., ed. The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. Fairfax, Virginia: AFCEA International Press, 1992.

Chairman, Joint Chiefs of Staff. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Joint Pub 6-0. Washington, D. C.: 1995.

_____. Doctrine for Joint Operations. Joint Pub 3-0. Washington, D. C.: 1995.

_____. Joint Doctrine for Command and Control Warfare (C2W). Joint Pub 3-13.1. Washington, D. C.: 1996.

_____. Joint Doctrine for Intelligence Support to Operations. Joint Pub 2-0. Washington, D. C.: 1995.

_____. Joint Vision 2010. Washington, D. C.: 1994.

Cohen, Eliot A. "A Revloution in Warfare." Foreign Affairs, March/April 1996, 37-54.

Cothron, Tony L. "Acheiving the Revolutionary Potential of Information Technology." Unpublished Research Paper, U. S. Naval War College, Newport RI: 1996.

Craft, Douglas W. An Operational Analysis of the Persian Gulf War. Carlisle Barracks, PA: Strategic Studies Institute, U. S. Army War College, 1992.

Cruickshank, Charles G. Deception in World War II. New York: Oxford University Press, 1980.

Devereaux, Christopher, LT. "Combat Leadership and the Media." Proceedings, July 1995, 62-65.

Drelling, Joseph S. "AirLand Battle and the Operational Commander's Information Requirements." Unpublished Research Paper, Fort Leavenworth, KS: School of Advanced Military Studies, U. S. Army Command and General Staff College, 1989.

Eisen, Stefan, Jr. "Netwar, It's Not Just For Hackers Anymore." Unpublished Research Paper, U. S. Naval War College, Newport RI: 1995

Fitzsimmons, James R. and Jan M. Van Tol. "Revolutions in Military Affairs." Joint Force Quarterly, Spring 1994, 24-31.

Hammes, Thomas X., LTCOL. "The Evolution of War: The Fourth Generation." Marine Corps Gazette, September 1994, 39-44.

Joint Military Operations Department, U. S. Naval War College. "Commander's Estimate of the Situation (CES) Workbook." Unpublished Class Manual (NWC 4111), U. S. Naval War College, Newport RI: 1996.

_____, U. S. Naval War College. "Elements of Operational Warfare." Unpublished Class Manual (NWC 4096), U. S. Naval War College, Newport RI: 1996.

_____, U. S. Naval War College. "Battlespace Information, Command and Control (C2), Operational Intelligence, and Systems Integration." Unpublished Class Manual (NWC 2127), U. S. Naval War College, Newport RI: 1996.

Key, Olen S. "The Impact of Information Warfare When Conducting Operational Deception." Unpublished Research Paper, U. S. Naval War College, Newport, RI: 1996.

Luoma, William M. "Netwar: The Other Side of Information Warfare." Unpublished Research Paper, U. S. Naval War College, Newport, RI: 1994.

Mann, Edward C. "Desert Storm: The First Information War?" Air Power Journal, Winter 1994, 4-13.

Morrison, David E. and Howard Tumber. Journalists at War. The Dynamics of News Reporting During the Falklands Conflict. London: Sage Publications, 1988.

Newell, Clayton R. The Framework of Operational Warfare. New York, NY: Routledge, 1991.

Nye, Joseph S., Jr and ADM William A. Owens. "America's Information Edge." Foreign Affairs, March/April 1996, 20-36.

Owens, William A., ADM. "A Report on the JROC and the Revolution in Military Affairs." Marine Corps Gazette, August 1995, 47-53.

Owens, William A., ADM. "Emerging System of Systems." Proceedings, May 1995, 35-39.

Peters, Ralph. "After the Revolution." Parameters, Summer 1995, 7-14.

Poole, James A. "The Challenge of Netwar for the Operational Commander." Unpublished Research Paper, U. S. Naval War College, Newport, RI: 1996.

Rather, Dan. "Honest Brokers of Information." Naval War College Review, Autumn 1995, 34-42.

Ryan, Julie, Gary Federici, and Tom Thurley. Information Support to Military Operations in the Year 2000 and Beyond: Security Implications. Alexandria, VA: Center for Naval Analyses, 1993.

Sandler, Stanley. "Army Psywarriors: A History of U. S. Army Psychological Operations." Special Warfare, October 1992, 18-25.

Scott, William B. "'Information Warfare' Demands New Approach." Aviation Week and Space Technology, March 13, 1995, 85-88.

Sexton, Joanne. "A Combatant Commander's Organizational View of Information Warfare and Command and Control Warfare." Unpublished Research Paper, U. S. Naval War College, Newport RI: 1995.

Sifry, Micah L. and Christopher Cerf, ed. The Gulf War Reader. History, Documents, Opinions. New York: Times Books, 1991.

Smith, Douglas V. "Military Deception and Operational Art." Unpublished Research Paper, U. S. Naval War College, Newport, RI: 1993.

Stevens, Peter F. "Early Disinformation Campaign." Military History, June 1992, 12+.

Stewart, John F., Mgen. "Commanders Pull Intelligence in Information Warfare Strategy." Signal, August 1994, 29-31.

Sullivan, GEN Gordon R. and James M. Dubik. War in the Information Age. Carlisle Barracks PA: Strategic Studies Institute, U. S. Army War College, 1994.

Summe, Jack N., Maj. "PSYOP Support to Operation Desert Storm." Special Warfare, December 1992, 6-9.

Train, Harry D. II. "An Analysis of the Falkland/Malvinas Islands Campaign." Naval War College Review, Winter 1988, 33-50.

U. S. Department of the Air Force. Cornerstones of Information Warfare. Washington, D. C.: HQ, Department of the Air Force, 1995.

U. S. Department of the Army. FM 100-6, Information Operations. Washington, D. C.: HQ, Department of the Army, 1996.

U. S. Department of Defense. Conduct of the Persian Gulf War. Final Report to Congress. v. 1. Washington, D. C.: U. S. Government Printing Office, 1992.

U. S. Department of Defense. Conduct of the Persian Gulf War. Final Report to Congress. v. 2. Washington, D. C.: U. S. Government Printing Office, 1992.

Van Creveld, Martin. The Transformation of War. New York, N. Y.: The Free Press, 1991.

Vego, Milan. "Fundamentals of Operational Design." Unpublished Class Manual (NWC 4104), U. S. Naval War College, Newport RI: 1996.

_____, Milan. "Operational Art." Unpublished Class Manual (NWC 4090), U. S. Naval War College, Newport RI: 1996.

_____, Milan. "Operational Factors." Unpublished Class Manual (NWC 4092), U. S. Naval War College, Newport RI: 1996.

Von Clausewitz, Carl. On War. Edited and Translated by Michael Howard and Peter Paret. Princeton, New Jersey: Princeton University Press, 1984.

Watson, Bruce W. and Peter M Dunn, ed. Military Lessons of the Falkland Islands War: Views from the United States. Boulder, Colorado: Westview Press, Inc., 1984.

Weidner, James H. "The People Side of Information Warfare." Unpublished Research Paper, U. S. Naval War College, Newport, RI: 1996.